Saskatchewan Cancer Agency

10C

Main points **182**

Introduction **183**

Audit conclusions and findings **183**

Better information technology processes needed 183

Timely annual report needed 184

Security of information technology data and system **184**

Objective and criteria 185

Audit conclusion 186

Key findings by criterion 186

Show management commitment to security 187

Protect systems and data from unauthorized access 188

Keep systems and data available for operation 191

Maintain the integrity of systems and data 192

Selected references **194**

Glossary **195**

Main points

Saskatchewan Cancer Agency (Agency) needs to improve its information technology (IT) policies and procedures. The Agency uses IT systems to support the delivery of patient care.

In 2008, we assessed the Agency's processes to secure its computers and data. We concluded the Agency did not have adequate processes to do so. Lack of adequate processes to secure (i.e., protect the confidentiality, integrity, and availability of) computer systems and data increase the risk of inappropriate disclosure of patients' information and inadequate patient care.

Also, the Agency needs to give its annual report to the Assembly by the date required by law.

Introduction

The Saskatchewan Cancer Agency (Agency) (formerly the Saskatchewan Cancer Foundation) conducts treatment, supportive care, research, education, prevention, and early detection programs for the control of cancer in Saskatchewan. The Agency operates cancer treatment centres in Regina and Saskatoon.

In 2008, the Agency had operating revenues of $81.0 million, operating expenses of $80.7 million, and surplus of $0.3 million. At March 31, 2008, it held assets of $49.0 million. The Agency's financial statements are included in its 2008 Annual Report.

Audit conclusions and findings

In our opinion, for the year ended March 31, 2008:

- **the Agency had adequate rules and procedures to safeguard public resources except for the matters reported in this chapter**
- **the Agency complied with the authorities governing its activities relating to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing except for the matters reported in this chapter**
- **the Agency's financial statements are reliable**

In this chapter, we also report the results of our audit of the Agency's processes to secure its information technology date centre, data network, and clinical management system.

Better information technology processes needed

In our 2007 Report – Volume 3 and prior reports, we recommended that the Saskatchewan Cancer Agency strengthen the preparation, approval, and implementation of information technology (IT) processes for its information systems that are based on a formal threat and risk analysis.

In March 2006, the Standing Committee on Public Accounts considered this matter and agreed with our recommendation.

We continue to recommend that the Saskatchewan Cancer Agency strengthen the preparation, approval, and implementation of information technology processes for its information systems that are based on a formal threat and risk analysis.

During the year, we did an audit of the Agency's IT security. We concluded that the Agency did not have adequate security policies and procedures. We report the results of that audit together with our recommendations later in this chapter.

Timely annual report needed

The Cancer Agency Act requires the Agency to give an annual report including financial statements to the Assembly according to *The Tabling of Documents Act, 1991.*

Under *The Tabling of Documents Act, 1991,* the Agency should have given its annual report to the Assembly on or before July 29, 2008. However, it has not yet done so. Accordingly, the Agency did not comply with *The Tabling of Documents Act 1991.*

1. We recommend that the Saskatchewan Cancer Agency give its annual report to the Legislative Assembly by the date required by *The Tabling of Documents Act, 1991.*

Security of information technology data and system

The Agency uses information technology (IT) systems to support the delivery of patient care. The Agency stores confidential patient data on its systems. The Agency plans to store additional electronic patient information by implementing a Clinical Management System (CMS). CMS has the ability for physicians to dictate and store notes in electronic format, integrate laboratory results, and store additional patient data including treatment information. When CMS is implemented, all data will be stored in one central location. CMS should help make patient information more accessible to staff, which could enhance the effectiveness of health care service delivery.

The Agency must protect the confidentiality and integrity of patient data. A loss of data could lead to inappropriate disclosure of a patient's medical records. Missing or inaccurate data could lead to inadequate patient care. The Agency uses its IT systems and data to provide patient services. Patient care could suffer if information in its systems is not available when needed.

Objective and criteria

The objective of our audit was to assess whether the Agency has adequate processes to secure its information technology data centre, data network, and clinical management system for the period from March 1, 2008 to August 31, 2008.

We used criteria to assess the Agency's processes. The criteria are based on the *Trust Services Criteria and Principles* authored by The Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants and on international standards, literature, and reports of other legislative auditors. The Agency's management agrees with the criteria.

The criteria, set out in the exhibit below, describe the key processes that we expected the Agency to use to secure its systems and data.

Exhibit 1 — Audit criteria

To secure its information technology data centre, data network, and clinical management system for the period from March 1, 2008 to August 31, 2008, the Agency should:

1. **Show management commitment to security**

   Responsibility for security is clearly defined
   Threat and risk assessments are performed
   IT planning supports security
   Management has approved security policies and procedures
   Management monitors security

2. **Protect systems and data from unauthorized access**

   User access controls protect its systems and data from unauthorized access
   Physical security controls protect its offices from unauthorized access

3. **Keep systems and data available for operation**

   System and data backups occur and are tested
   Disaster recovery plans are in place and are tested

4. **Maintain the integrity of systems and data**

   Change management processes exist and are followed
   Computer operation processes exist and are followed

Throughout our audit, we followed *The Standards for Assurance Engagements* established by The Canadian Institute of Chartered Accountants.

Audit conclusion

The Saskatchewan Cancer Agency did not have adequate processes to secure its information technology data centre, data network, and clinical management system for the period from March 1, 2008 to August 31, 2008.

We describe our expectations for each criterion and recommendations in the following section.

Key findings by criterion

We describe below what we expected (in italics) and key findings for each criterion.

Show management commitment to security

Management commitment includes setting up an organizational structure that clearly defines who is responsible for security. We expected a member of the Agency's senior management would lead an information technology (IT) group. Management should effectively monitor contractors who perform work on its behalf. Commitment also includes implementing and monitoring compliance with security policies and procedures.

The Agency has an organizational structure that defines who is responsible for the security of information. A senior manager leads the IT division. The Agency has a team of eight IT staff who manage, maintain, and monitor its systems and data.

The Agency prepared an IT operational plan for 2008-09. The plan identifies its strategic themes and priorities and sets out objectives and initiatives for each priority.

The Agency has developed policies based on a risk assessment. The Agency's senior management has approved some of the IT policies. Management told us the Agency plans to approve all IT policies by December 31, 2008.

The Agency has not implemented all of its new policies. Nor has it established procedures for all policies. For example, the Agency has developed a backup policy, but has not documented its backup and recovery procedures. Also, implementation generally includes providing awareness training to all staff. The Agency needs to do so. The Agency also needs processes to monitor and enforce compliance with policies and procedures.

The Agency uses the IT unit of the Ministry of Health as a service provider to provide network management, security, and data transmission controls. The Agency met with the service provider monthly and received some information on planned changes and work plans. However, the Agency did not know if the service provider's security controls were adequate. Weaknesses at the service provider could adversely affect the security of the Agency systems and data.

The service provider did not provide all security services that the Agency had expected. For example, the service provider did not monitor firewalls on the Agency's behalf. The Agency did not monitor the service provider to ensure it received all required services. As a result, the Agency did not know if its systems are protected from unauthorized users. Nor did it know if data transmitted on the service provider's network was secure.

2. We recommend the Saskatchewan Cancer Agency monitor its information technology service provider to ensure its systems and data are adequately protected.

Management has advised that the service provider is working on addressing the need for providing assurance information for all of its clients. Management has also advised that the Agency began directly monitoring its firewalls in September 2008 and the service provider is in the process of installing a new intrusion detection system (IDS).

Protect systems and data from unauthorized access

We expected the Agency to have adequate physical access and user access processes to protect the systems and data from unauthorized access.

Good physical control means protecting IT infrastructure from harm. Physical access controls protect all computers and network devices from unauthorized access. For example, security controls should physically prevent unauthorized users from entering a data centre.

User access controls ensure only approved people or processes can use an IT system. A common example of a user access control is a username and a password. The username identifies the user and the password grants access.

Protecting systems from unauthorized access is more critical with the increased use of the Internet, automated processes, and multiple offices. The Agency should protect its data by configuring, updating, and monitoring its systems against security threats.

The Agency uses locked rooms to protect its computers and related computer equipment that run the network and store patient data. The

rooms are alarmed and monitored 24 hours daily. Batteries provide backup power and generators are available if needed.

The Agency has documented processes for granting and removing user access to its IT systems and data. However, the Agency did not adequately comply with its processes during the audit period. Staff no longer employed by the Agency continued to have access to systems and data. Also, the Agency did not remove or disable administrator access privileges for consultants who had not recently used their accounts for accessing the Agency's network. The Agency should perform regular tests to check that only valid users have access to its systems and data. Management informed us that the Agency has now strengthened its processes for granting and removing user access.

The Agency needs to consistently follow its password standards. For example, over 100 network accounts did not have passwords set to expire. Also, some administrator passwords were over 2 years old. Management informed us that the Agency has rectified the situation.

3. We recommend the Saskatchewan Cancer Agency follow its policies for accessing computer systems and data.

The Agency uses a wireless network at its cancer centres in Regina and Saskatoon. Medical staff access and modify patient information using the wireless network.

The Agency did not adequately configure its wireless networks. The Agency did not restrict wireless access to specific computers. Nor did it monitor attempts to access its wireless network. As a result, attempted or successful security breaches would not be detected. The Agency did not implement firewalls between the wireless access points and its network.

The Agency used encryption to protect the wireless data. However, the wireless encryption used is now several years old and is vulnerable to attack because its shortcomings are well known on the internet.

We tested the wireless network in Regina. The wireless signal is accessible from outside the cancer centre and in public areas such as a coffee shop. During our audit, we successfully broke the Agency's encryption key. The Agency was immediately informed that its wireless

system is vulnerable to outside attack. An inappropriate user could breach the Agency's wireless systems using a laptop and software tools freely available on the internet.

Knowing the encryption key would not immediately grant access to the Agency's systems and data. Access to the network requires a user to enter a valid username and password. However, the Agency did not lock user accounts after a specified number of failed logon attempts. Also, the Agency did not monitor failed access attempts to its network. As a result, a potential intruder could run automated tools to obtain a valid network username and password. These tools are widely available on the internet. The Agency would not know if an intruder attempted or successfully breached its network.

4. We recommend the Saskatchewan Cancer Agency adequately protect its wireless computer systems against unauthorized access.

Management told us that on October 8, 2008 the replacement of the Agency's wireless system had been completed. Management told us that the Agency has enforced account locking after a specified number of failed password attempts and now monitors failed access attempts to the network.

Computer vulnerabilities are often detected after a system is in use. The process of updating computers for known weaknesses is referred to as patching. Patching computers regularly prevents unauthorized users from exploiting known vulnerabilities.

The Agency has patched most of its computers. However, the Agency did not adequately patch all computers used to protect its network and access patient data. The Agency needs to patch its computers on a timely basis to protect itself from security threats.

5. We recommend the Saskatchewan Cancer Agency protect its computer systems and data by updating (patching) its computers against known security weaknesses.

The Agency used some strong configuration settings on its computers. For example, password complexity and minimum password length were

enforced for all users. Also, the Agency did log some security events such as application errors. However, some configuration settings were weak or not enforced. For example, many passwords were not set to expire and user accounts do not lock after a specified number of failed logon attempts.

As we stated earlier, the Agency used a service provider to monitor its firewalls. The Agency knew before the start of the audit period, that the service provider was not monitoring the firewalls. However, the Agency did not monitor the firewall logs itself.

The Agency did not log or monitor access attempts to its network. The Agency did not have a process to detect potential inappropriate activity on its key servers or network. Timely review of logs would help identify potential or successful security attacks.

6. We recommend the Saskatchewan Cancer Agency protect its information technology systems and data by adequately monitoring its systems and data for security threats.

Keep systems and data available for operation

We expected the Agency *to have adequate processes to ensure its systems and data are available for operation when needed.*

Even with good backup and recovery procedures, the Agency may not be able to continue its operations if a major problem occurs. Therefore, the Agency should have a contingency plan to recover operations in the event of a disaster like a fire or flood. This includes building capacity, when cost effective, into systems so a disaster in one location will not cause applications to quit running at other locations where employees are still able to work.

The Agency needs to document backup and recovery procedures for its systems and data. The backup and recovery procedures should define data requirements, frequency, offsite storage needs, and recovery processes.

The Agency developed a disaster recovery plan. The disaster recovery plan outlines roles and responsibilities of staff, scope and objective of the

plan, site information, recovery requirements, and detailed recovery procedures for significant servers.

The Agency tested some of its disaster recovery procedures in June 2007. The Agency was not able to recover its systems in the time required. Management told us that the Agency has retested the disaster recovery procedures. However, we did not see evidence of such test or its results.

The Agency did not test whether its data would be available to meet its recovery point objectives. For example, the Agency required restoration of some systems and data in 24 hours. The recovery time objective of 24 hours would require the Agency to store backup tapes offsite daily. The Agency stored backup tapes offsite weekly. If a disaster had occurred and the on-site backup tapes were destroyed, the data restored could be up to seven days old and the Agency would not be able to meet its data recovery requirements.

Management told us that while not all of the planned recovery point objectives were met, the Agency's most critical system, CMS, is backed up on an hourly basis.

The Agency successfully restored individual systems and data upon request (for example, when files were lost or computers replaced). However, without an adequately tested plan, the Agency does not know if it could restore all systems and data in the event of a disaster.

7. We recommend the Saskatchewan Cancer Agency adequately test its disaster recovery plan.

Management told us that the Agency plans to perform a disaster recovery test in October 2008.

Maintain the integrity of systems and data

We expected the Agency *to have processes for maintaining the integrity of client systems and data by implementing adequate configuration, update, monitoring, and IT operation processes. Adequate processes require approving and testing system changes before implementation.*

The Agency should ensure that it has adequate processes for running and maintaining its computers.

The Agency needs to strengthen its processes for configuring, updating (patching), and monitoring its computers. The Agency needs adequate computer operating processes to keep its computers secure. We describe these findings and recommendations earlier under the heading "Protect systems and data from unauthorized access."

The Agency has adequate processes for managing changes to its CMS. The Agency documented, approved, and tested changes to the CMS application prior to implementation.

Selected references

Canadian Institute of Chartered Accountants (CICA) & American Institute of Certified Public Accountants (AICPA). (2007). For Security, Availability, Processing Integrity, Confidentiality, and Privacy. (Including WebTrust® and SysTrust™). In *Trust services principles and criteria*. Toronto: Author. http://www.cica.ca/index.cfm/ci_id/38256/la_id/1. (25 Apr 2008)

Canadian Institute of Chartered Accountants. (CICA). (1998). *Information technology control guidelines*. Toronto: Author.

Information Systems Audit and Control Foundation. (2005). *CoBiT4.0*. Rolling Meadows, IL: Author.

International Organization for Standardization. (2005). ISO/IEC 27002:2005(E). *Information technology – Code of practice for information security management; 2nd Edition*. Geneva: Author.

IT Governance Institute. (2006). IT Control Objectives for Sarbanes-Oxley: *The role of IT in the design and implementation of internal control over financial reporting, 2nd Edition*. Rolling Meadows, IL: Author.

Glossary

Account—A unique identity set up on a computer or network that allows access to specific systems and data.

Application—A software program. This includes programs such as word processors, spreadsheets, database programs, accounting programs, etc.

Backup (noun)—A copy of systems or data to be used when the originals are not available (e.g., because of loss or damage).

Configure—To set up or arrange in order to achieve a specific purpose (e.g., maximize security).

Data centre—A central location for computer network hardware and software, especially storage devices for data.

Disaster recovery plan—A plan for an organization to restore necessary IT services in the event of an emergency or disaster. A disaster recovery plan is one part of a larger, organization-wide business continuity plan.

Encryption—A method of putting information in code so that only authorized users will be able to see or use the information.

Firewall—A piece of hardware or software intended to restrict or block access to a network or computer. Firewalls can be set up to only allow certain types of data through.

Intrusion detection system (IDS)—software and/or hardware designed to detect a security breach by identifying inappropriate access or changes taking place within a network or computer.

IT infrastructure—An organization's computer and network assets.

Network—A group of computers that communicate with each other.

Patch—An update to a computer program or system designed to fix a known problem or vulnerability.

Physical access controls—The controls in place at an organization that restrict unauthorized people from gaining physical access to computers or network equipment. Examples include locked doors and cabinets, and video surveillance systems.

Recovery point objective—In disaster recovery, the intended point in time before an emergency or disaster to which systems and data can be restored. For example, if backups of data are done every 4 hours, and an emergency or disaster occurs 3 hours after the last backup, then 3 hours of data may not be recoverable. The recovery point objective in this case is 4 hours, and represents the maximum amount of data that management is prepared to lose because of a disaster.

Recovery time objective—In disaster recovery, the point in time after an emergency or disaster by which management plans to have systems and data available. If the recovery time objective for a system is 24 hours, management plans to have that system operational within 24 hours after an emergency.

Server—A computer that hosts systems or data for use by other computers on a network.

User access controls—The controls in place at an organization to restrict use of systems or data to those who have been authorized. These include physical controls such as locked doors or cabinets, as well as computer and network controls such as establishing accounts with specific access rights, requiring passwords, etc.